Supporting Finance Cyber Resilience and Recovery

Financial services organizations have been an expert in dealing with cyber threats, yet they are not immune to the impact of cyber events. This infographic outlines the key steps to ensure financial services cybersecurity resilience and recovery.

1. **Prevention**: Building a robust security infrastructure to prevent cyber attacks.
2. **Detection**: Identifying potential threats and vulnerabilities in real-time.
3. **Response**: Quickly and effectively responding to cyber incidents.
4. **Recovery**: Ensuring business continuity and minimizing downtime.

A Snapshot of Key Financial Services Cybersecurity Jobs

- **Cyber Security Analyst**: Monitors and investigates potential security breaches.
- **Penetration Tester**: Tests the security of a computer system.
- **Cyber Security Architect**: Designs and implements security measures.

Practical Strategies for Upgrading Your Financial Cyber Resilience

- **Implement Multi-Factor Authentication (MFA)**: Enhances security by requiring multiple forms of verification.
- **Stay Updated with Cybersecurity Best Practices**: Keep your systems and applications up-to-date with the latest security patches.
- **Regularly Audit Cybersecurity Policies**: Ensure compliance and address any vulnerabilities.
- **Train Employees on Cybersecurity Awareness**: Educate employees on recognizing and responding to cyber threats.

Cascaded
cascaded.com | 888.234.5678 | support@cascaded.com